

ASPECT® v3.08.00

Summary

ASPECT software has been updated to include a BACnet Operator Workstation (B-OWS) - ASPECT-SUPERVISOR, Security Enhancements, Routing and Navigation improvements, along with General Usability improvements.

Features

ASPECT-SUPERVISOR (BTL-CERTIFIED BACNET WEB INTERFACE)

ASPECT v3.08.00 includes ASPECT-SUPERVISOR, a new BTL-certified BACnet Operator Workstation (B-OWS) feature for BACnet discovery, browsing and property view/edit.

Note: This feature is available on *new* NEXUS and ASPECT-Enterprise devices only. Existing devices upgraded to v3.08.00 and new MATRIX variants will not include the B-OWS feature.

To access ASPECT-SUPERVISOR: log in to `ngAdmin` as a user that is part of the `SUPAdmin` group, then click `Utilities > Aspect Supervisor`. See [Help Docs](#) in the app for more information.

The screenshot displays the ASPECT-SUPERVISOR web interface. At the top, it shows the ABB logo, the title 'ASPECT-SUPERVISOR', and the source device name '192.168.4.112 : 47809'. The interface is divided into several sections:

- Discovery Scope:** Includes a dropdown menu set to 'Global', 'High Limit' and 'Low Limit' both set to '-1', and a 'Refresh' button.
- Device List Table:** A table with columns for Device Id, Device Name, IP Address, SNET, and SADR. The first row is highlighted, showing Device Id 305, Device Name ASPECT-SUPERVISOR, and IP Address 192.168.4.112.
- Property Browser:** Shows the selected device 'Device 305 PR 19' and an 'Object List' with a search field. The 'Device' object is expanded to show 'Device_305' and 'NetworkPort'.
- Property Editor:** A table with columns for Property Name and Property Value. It lists various properties such as ObjectIdentifier, ObjectName (ASPECT-SUPERVISOR), ObjectType (Device), MaxSegmentsAccepted (32), APDUsegmentTimeout (6000), LocalDate (9/6/2023), LocalTime (07:14:46), Location (Atlanta, USA), Description (ASPECT-SUPERVISOR 4112), ProfileName (I71-B-OWS), SerialNumber (1234), SystemStatus (Operational), VendorName (ABB), VendorIdentifier (I71), and ModelName (ASPECT-SUPERVISOR).

Note: ASPECT Device IDs and internal network numbers must be unique on your BACnet network in order for ASPECT-SUPERVISOR B-OWS to run smoothly. Supervisor B-OWS will be configured with a unique Device ID and network number automatically on first launch. These unique IDs are generated using the last 2 octets of the devices IP address. Device ID and network number are configurable after first launch.

However, ASPECT routers on ASPECT-Enterprise, NEXUS and MATRIX devices may need to be configured with unique BACnet Device Instance Number and BACnet Internal Network Number (WebUI > Communication Setup > BACnet > BACnet Settings).

SECURITY ENHANCEMENTS

- The appearance of the ASPECT login page has changed:

- Single sign-on has been implemented for ASPECT Apps so that a login to ngAdmin will also permit access to System Administration (WebUI) and ASPECT-SUPERVISOR (where user/group permissions allow).

Note: Logging out of one application will log the same user out of *all* applications in the browser.

- By default Users with a “weak” password will be required to change their password at next login after 3.08.00 upgrade. This is configurable in WebUI > Authentication Configuration > Security Level.
- The factory default credentials `aamuser/default` and `guest/guest` are now required to be changed before upgrade to v3.08.00 is permitted.
- The factory default credentials `aamuser/default` and `guest/guest` are now required to be changed at the first login to any ASPECT target device.
- Changing a password in one application will result in a password change across all applications (where passwords are synchronized between applications to begin with).
- Session expiry and password rules can now be configured in WebUI > Authentication Configuration.
- Users can now change their own passwords in ngAdmin (user icon drop-down menu > User Preferences).

Resolved Issues

- ASP-6181 Authenticated proxy from ngAdmin to B-OWS has been added on ASPECT-Enterprise / NEXUS platforms.
- ASP-6225 ASPECT WebUI (System Administration) link is now visible only to authorized users, and access is "proxy" authenticated.
- ASP-6226 Aspect Supervisor (B-OWS) link is now visible only to authorized users and access is "proxy" authenticated.
- ASP-6262 Passwords can no longer be added to the Security/Auth debug logs.
- ASP-6264 Authenticated proxy configuration has been implemented for the Centos 6 version of Apache.
- ASP-6266 An app-selection dropdown has been added to the ngAdmin login page.
- ASP-6295 Session idle timeouts have been implemented in ngAdmin.
- ASP-6296 Session idle time is now updated for the user across all apps.
- ASP-6303 Copy & Paste of credentials has been disabled on login page.
- ASP-6307 Authentication Configuration page has been added to WebUI - (session expiry rules, password rules, etc.).
- ASP-6318 Graphics Preview has been updated to work with the new authentication mechanisms.
- ASP-6327 The "default" username & password has been removed from new deployment targets in ASPECT-Studio.
- ASP-6335 Remove weak TLS ciphers from ASPECT.

ROUTING AND NAVIGATION IMPROVEMENTS

1. The following routing/navigation changes will take effect with 3.08.00:
 - The default “landing page” for ASPECT is now ngAdmin. This is the application that will be reached if a bare IP address or hostname is entered (without any additional URL path). System Administration (WebUI) and ASPECT-SUPERVISOR can be reached from links under Utilities menu in ngAdmin.
 - The URLs for the WebUI (System Administration) application now include `/admin` at the start of the path e.g. <http://192.168.4.100/admin/setup.php>. This means that existing local bookmarks may need to be updated.

Resolved Issues

- ASP-6086 The project name has been added to the ngAdmin login page.
- ASP-6315 The Manage Port option has been removed from the WebUI interface (Web Server SSL Configuration).
- ASP-6317 Upgrade will now stop if the Use First Instance option is selected.

GENERAL USABILITY

Resolved Issues

- ASP-6209 A diagnostic tool has been added to capture traffic on any port.
- ASP-6247 Connection & read timeouts have been added to ASPECT XPath Reader to prevent blocking by the process.
- ASP-6292 MATRIX variant labelling (MATRIX/Matrix-Max/MATRIX-2) has been clarified on login pages and WebUI.
- ASP-6367 All ASPECT UI sections now have uniform headers and branding.
- ASP-6403 Network device changes (e.g. docking station) no longer cause an issue with ASPECT-Studio license.

Customer Impact

Customers are recommended to update when convenient. However, the following should be noted:

1. The factory default credentials **must** be changed before upgrade to v3.08.00 is permitted.
2. The v3.08.00 upgrade process will only be successful if the default option **Aspect Target Admin UI** is selected on the **Web Server SSL Configuration WebUI** page.
3. By default, Users with a “weak” password will be required to change their password at next login after 3.08.00 upgrade. This is configurable in **WebUI > Authentication Configuration > Security Level**
4. The new **ASPECT-SUPERVISOR** feature (BTL-certified “B-OWS”) will be present on on *new* NEXUS and ASPECT-Enterprise devices only. Existing devices upgraded to v3.08.00 and new MATRIX variants will not include the B-OWS feature.
5. After applying an ASPECT license in **WebUI** (System Administration), a **System Restart** is required (see **System Services** menu).
6. While most **ngAdmin** features will work on an **IOS (Apple)** device, full support is not guaranteed.

Note: Since v3.07.00, it is possible to open or close IP ports on ASPECT devices (**WebUI > Communication Setup > IP Port Administration**).

- *For existing devices*, it is recommended that all ports should be closed for increased security. Note that upgrading an existing device to v3.08.00 will not close any ports, so it is recommended that any unnecessary ports are manually closed.
- *For new devices*, all unnecessary ports will be closed by default, but you can browse the device using HTTPS (port 443 – always open). During project deployment, you will need to temporarily open ports 80 and 7226.